SHRegGetPath

The destination string buffer must be long enough to hold the return file path.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4044 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Malicious Input
• Path spoofing or confusion problem</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Buffer Overflow
• Unconditional</td></tr>
<tr><td><b>Software Context</b></td><td>• File Path Management</td></tr>
<tr><td><b>Location</b></td><td>• shlwapi.h</td></tr>
<tr><td><b>Description</b></td><td>The destination string buffer for SHRegGetPath() must be long enough to hold the return file path. Otherwise, buffer overflows will occur.
SHRegGetPath() retrieves a file path from the registry, expanding environment variables as needed.</td></tr>
<tr><td><b>APIs</b></td><td><table>
<tr><th>FunctionName</th><th>Comments</th></tr>
<tr><td>SHRegGetPath</td><td></td></tr>
<tr><td>SHRegGetPathA</td><td>ASCII implementation</td></tr>
<tr><td>SHRegGetPathW</td><td>Unicode implementation</td></tr>
</table></td></tr>
<tr><td><b>Method of Attack</b></td><td>Buffer Overflow</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table>
<tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr>
<tr><td>Whenever SHRegGetPath() is called.</td><td>The fourth parameter, pszPath, must be at least MAX_PATH characters in length.</td><td>Effective.</td></tr>
</table></td></tr>
<tr><td><b>Signature Details</b></td><td>DWORD SHRegGetPath(
HKEY hkey,
LPCTSTR pszSubkey,
LPCTSTR pszValue,
LPTSTR pszPath,
DWORD dwFlags</td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	);

Examples of Incorrect Code	`TCHAR pszPath[15]; // Buffer is too small`
	`HKEY hkey;`
	`[...] // set hkey to a handle to a key that is currently open, or a registry root key.`
	`DWORD result = SHRegGetPath(`
	`hkey,`
	`TEXT("MySubKey"),`
	`TEXT("MYValue"),`
	`pszPath,`
	`0`
	`);`
	`if (result != ERROR_SUCCESS) { /* handle error */ }`

Examples of Corrected Code	`TCHAR pszPath[MAX_PATH]; // Buffer is properly sized`
	`HKEY hkey;`
	`[...] // set hkey to a handle to a key that is currently open, or a registry root key.`
	`DWORD result = SHRegGetPath(`
	`hkey,`
	`TEXT("MySubKey"),`
	`TEXT("MYValue"),`
	`pszPath,`
	`0`
	`);`
	`if (result != ERROR_SUCCESS) { /* handle error */ }`

Source Reference	
Recommended Resources	• MSDN reference for SHRegGetPath[2] • MSDN reference for Registry Functions[3]
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com